Michael A. McShane, SBN 127944
Mark E. Burton, Jr., SBN 178400
AUDET & PARTNERS, LLP
711 Van Ness, Suite 500
San Francisco, CA 94102-3229
Tel: 415.568.2555 | Fax: 415.568.2556
mmcshane@audetlaw.com
mburton@audetlaw.com

Caleb Marker, SBN 269721
ZIMMERMAN REED LLP
2381 Rosecrans Avenue, Suite 328
Manhattan Beach, CA 90245
Tel: 877.500.8780 | Fax: 877.500.8781
caleb.marker@zimmreed.com

*Attorneys for Plaintiff and the Class*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL GONZALES, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

UBER TECHNOLOGIES, INC., a Delaware corporation, UBER USA, LLC, a Delaware limited liability company, RAISER-CA, a Delaware limited liability company, and DOES 1-10, inclusive,

Defendants.

CASE NO.: 3:17-CV-02264

**SECOND AMENDED COMPLAINT (CLASS ACTION)**

1. Violation of the Stored Communications Act (18 U.S.C. § 2701)
2. Violation of California's Computer Data Access and Fraud Act (Cal. Penal Code, § 502)
3. Violation of the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 *et seq.*)
4. Invasion of Privacy (Cal. Const. Art. I, § 1)

(Jury Trial Demanded)

Plaintiff Michael Gonzales, individually and on behalf of all persons similarly situated, alleges the following by and through the undersigned attorneys.

**NATURE OF THE ACTION**

1. Plaintiff Michael Gonzales ("Plaintiff") brings this action on his own behalf and as a class action for the benefit of a Class consisting of Lyft drivers whose electronic communications and whereabouts were accessed, monitored, and/or transmitted by Defendants and used to gain an unfair advantage in the market at the expense of the Plaintiff and Class.

2. Plaintiff and the Class seek injunctive relief and damages caused by Defendants' unlawful invasion of privacy and access of electronic communications in violation of the Federal Stored Communications Act (the "SCA"), the California Unfair Competition Law (the "UCL"), the California Computer Data Access and Fraud Act (the "CDAFA"), and invasion of privacy.

3. Lyft provides technology that operates in a fashion similar to a taxi company's dispatch system. A rider requests a ride using a software application on his or her smart phone (the "Lyft Rider App"). The locations of nearby Lyft drivers are displayed to the rider as dots on a map, along with the estimated price and wait time for arrival once the ride request is submitted.

4. Drivers also use a Lyft app (the "Lyft Driver App"). When a driver is ready to accept work, the driver swipes a switch on the Lyft Driver App, directing the Lyft Driver App to continuously transmit and store the driver's geolocation data and his or her willingness to accept specific types of rides (*i.e.*, Shared, Lyft, Lyft XL, Lux, Lux Black, Lux Black XL) to servers maintained by Lyft. Lyft, acting as the drivers' agent, then forwards the information to Lyft's riders.

5. Lyft stores driver's personal data, but ultimately the data belongs to the respective individual. That is, under Lyft's Terms of Service/Privacy Policy, the data is licensed to Lyft, but drivers like Plaintiff and Class members retain full ownership of their own personal data.

6. Uber offers technology that competes with the Lyft Application (Lyft Rider App and Lyft Driver App herein referred collectively as the "Lyft App"), that in all ways relevant to this litigation functions identically to Lyft's business model.

7. Uber operates in the same geographic regions as Lyft. Some drivers even perform transport services through the two platforms simultaneously.

8. Seeking a competitive advantage over Lyft, Uber developed and deployed spyware, code-named "Hell," that allowed it to gain unauthorized access to information that was transmitted through and stored on Lyft's computer systems and servers. The Hell spyware extracted information from Lyft by posing as Lyft customers in search of rides. Using Hell, Uber's employees, contractors, and/or agents were able to harvest the data transmitted by Lyft drivers, including their locations and Lyft ID's. Each Lyft ID is unique, akin to a social security number, allowing Uber to track Lyft drivers' locations and movements over time, in violation of the Lyft App's Terms of Service.

9. Upon information and belief, Uber repeated this process millions of times using the Hell spyware from 2014 through 2016 to gain an unfair advantage in the market place at the expense of Plaintiff and Class.

10. Upon information and belief, Uber combined the data harvested by Hell with Uber's internal records (such as historical location data) to, among other things, identify Lyft drivers who also worked for Uber. Essentially, Uber was looking for overlap between its location data and Lyft's so that it could inundate drivers who used both platforms with work, encouraging drivers to use Uber's platform exclusively, and thus harm drivers who only used the Lyft platform. By reducing the supply of Lyft drivers, Lyft customers saw increased wait times, which ultimately led Lyft-only drivers to experience decreased overall earnings, decreased earnings per fare, cancelled fares, and a decrease in the quantity of fares per shift.

11. Plaintiff and Class Members used the Lyft Driver App during the time that Uber deployed the Hell spyware. Plaintiff and Class Members sent communications through the Lyft Driver App to prospective passengers notifying them of their locations, their availability to provide transportation services, and the cost of transportation at the time the communications were accessed by the Hell spyware. Using this information, the Defendant was able to gain an unfair advantage over the market by manipulating drivers and the fare amount that were collected in the market place.

12. Courts have confirmed that tracking the GPS of an individual "chills associational and expressive freedoms." *United States v. Jones*, 565 U.S. 400, 413 (2012) (Sotomayer, J., concurring). "…GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered

discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* (quoting *United States v. Cuevas–Perez,* 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

13. Most recently, the Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), affirmed this reasoning by finding that the government's acquisition of defendant's historical cell-site location information ("CSLI") from wireless carriers was an unreasonable search under the Fourth Amendment. This is because "[t]he ability to chronicle a person's past movements through the record of his cell phone signal… is detailed, encyclopedic, and effortlessly compiled." Because individuals have reasonable expectation of privacy in the whole of their physical movements, individuals "maintain[] a legitimate expectation of privacy in the record of [their] physical movements as captured through CSLI." *Id.* at 2217. "Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 2218.

14. The same principles identified by the Supreme Court apply to a corporation monitoring the movements of a competitor's workers through surreptitious spyware.

15. Uber has never publicly acknowledged the use of its Hell spyware but did not deny its existence when asked to respond to news reports.

16. Nor has Uber notified Class Members that their personal information was harvested and compromised by the Hell spyware, or made any attempts to rectify the illegal and/or dishonest practices by way of deleting personal geolocation or confirming the cessation of the spyware program.

**THE PARTIES, JURISDICTION AND VENUE**

17. Plaintiff brings this action pursuant to §§ 2701 through 2712 of title 18 of the United States Code also known as the Stored Communications Act ("SCA").

18. This Court has original jurisdiction over federal law claims pursuant to 28 U.S.C. §§ 1331 and 1337.

19. This Court also has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367, as those claims are so related to the claims in the action within the Court's original jurisdiction that they form part of the same case or controversy.

20. Plaintiff is an adult California resident.

21. Plaintiff used the Lyft Driver App and worked as a Lyft driver from 2012 until approximately November 2014. Plaintiff may work as a Lyft Driver in the future.

22. During the time that Plaintiff used the Lyft Driver App, he drove passengers in the San Francisco Bay Area, including, but not limited to, the counties of San Francisco, Santa Clara, and San Mateo.

23. At no time has Plaintiff Gonzales ever worked for any of the Defendants or any subsidiaries or affiliates of any of the Defendants.

24. At no time has Plaintiff Gonzales ever executed any contract or arbitration agreement with any of the Defendants.

25. Defendant Uber Technologies, Inc. is a Delaware corporation that maintains a principal place of business at 1455 Market Street, Fourth Floor, San Francisco, California 94103.

26. Defendant Uber USA, LLC is a Delaware limited liability company and maintains a principal place of business at 1455 Market Street, Fourth Floor, San Francisco, California 94103.

27. Defendant Rasier-CA, LLC is a Delaware limited liability company and maintains a principal place of business at 1455 Market Street, Fourth Floor, San Francisco, California 94103.

28. Together, Defendants Uber Technologies, Inc., Uber USA, LLC, and Rasier-CA, LLC are referred to collectively as the "Defendants" or "Uber."

29. Lyft operates as Uber's main competitor in the United States.

30. Plaintiff does not know the true names and capacities of the defendants sued herein as Does 1 through 10 ("Doe Defendants"), inclusive, and therefore sues said Doe Defendants by fictitious names. Plaintiff, based on information and belief, alleges that each of the Doe Defendants is contractually, strictly, negligently, intentionally, vicariously liable and/or otherwise legally responsible in some manner for the acts and omissions described herein. Plaintiff will amend this

Complaint to set forth the true names and capacities of each Doe Defendants when the same are ascertained.

31. Plaintiff, based on information and belief, alleges that Uber and Doe Defendants 1 through 10, inclusive, and each of them, are and at all material times have been, the agents, servants or employees of each other, purporting to act within the scope of said agency, service or employment in performing the acts and omitting to act as alleged herein. Each of the Defendants named herein are believed to, and are alleged to, have been acting in concert with, as employee, agent, co-conspirator or member of a joint venture of, each of the other Defendants, and are therefore alleged to be jointly and severally liable for the claims set forth herein, except as otherwise alleged.

32. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendants reside in this District, conduct substantial business in this District, and the Plaintiff was a victim of Defendants' surveillance while working as a Lyft driver in this District.

33. Venue is also proper in this District because the Defendants received, managed, accessed, used, and transmitted communications collected in this District.

34. In connection with the acts and conduct complained of below, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including the internet, or made such use possible.

## CLASS ACTION ALLEGATIONS

35. Plaintiff brings this action against Defendants pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and all other persons similarly situated. Plaintiff seeks to represent the following classes:

**The National Class**

> All individuals who (1) worked as drivers in the United States, and (2) used the Lyft App, (3) while not working for Uber, and (4) had their private information, including their whereabouts, obtained through Uber's access of computer systems operated by the Class or by Lyft on behalf of the Class (the "Class").

**The California Subclass**

All individuals who (1) worked as drivers in California, and (2) used the Lyft App, (3) while not working for Uber, and (4) whose private information and whereabouts were obtained through Uber's access of computer systems operated by Lyft or the Class (the "California Subclass").

36. The "Class Period" dates back four years (or the length of the longest applicable statute of limitations for any claim asserted) and continues through the present and the date of judgment.

37. Excluded from the Classes are: (a) any officers, directors or employees of Uber or Lyft; (b) any judge assigned to hear this case (or spouse or family member of any assigned judge); (c) any employee of the Court; and (d) any juror selected to hear this case. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

38. All requirements for class certification in Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2) or 23(b)(3) (or any other applicable state or federal rule of civil procedure) are satisfied with respect to the Class. Plaintiff and Class Members were injured by Uber's deployment and use of its Hell spyware. Uber subjected Plaintiff and each Class Member to the same unfair, unlawful, and deceptive practices and harmed them in the same manner.

39. Numerosity: The proposed classes are so numerous that it would be impracticable to join all members. According to public reports, more than 315,000 individuals have driven for Lyft in the United States and perhaps 60% of those individuals have also driven for Uber.[1] Thus, the number of Class Members in the National Class who never worked for Uber may number 126,000 or more. Common sense dictates that thousands of those individuals are California residents.

[1] https://www.theinformation.com/ubers-top-secret-hell-program-exploited-lyfts-vulnerability

40. Ascertainability: The community of interest among Class members in the litigation is well defined and the proposed classes are ascertainable from objective criteria. If necessary to preserve the case as a class action, the court itself can redefine the Class. Both Uber and Lyft maintain highly detailed, accurate, and easily accessible databases of their respective drivers, and individual Class Members have access to accurate records that can confirm their membership in the proposed Class(es).

41. Plaintiff's claims are typical of the Class, as Plaintiff and all other Class Members were injured in exactly the same way by the Hell Spyware's unauthorized collection, use, and/or transmission of their personal information and electronic communications allowing the Defendant to manipulate the marketplace to gain an unfair competitive advantage at the expense of the Class causing all Class Members concrete economic losses.

42. Plaintiff will fairly and adequately represent the Class' interests and has retained counsel competent and experienced in class action and complex litigation.

43. Plaintiff has no interests that are contrary to or in conflict with those of the Class.

44. A class action is superior to other available methods for the fair and efficient adjudication of this controversy under the acts described below. Given the nature of these claims, the expense and burden of individual litigation make it virtually impossible for the Class Members to individually seek redress for the unlawful conduct alleged.

45. Plaintiff knows of no foreseen difficulty in the management of this litigation that would preclude its maintenance as a class action.

46. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual Class Members. Among the questions of law and fact common to the Class are:

a. Whether Defendants' acts as alleged herein violated the SCA;

b. Whether Plaintiff and members of the Class are entitled to compensatory damages, as well as statutory and punitive damages pursuant to the SCA;

c. Whether Defendants' acts as alleged herein constituted invasions of Plaintiff's and Class' privacy;

d. Whether Defendants' acts as alleged herein constituted violations of the UCL; and

e. Whether Plaintiff and members of the Class are entitled to restitution, as well as injunctive relief pursuant to the UCL.

47. Plaintiff brings this action under Rule 23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to all members of the Class, thereby making final relief concerning the Class as a whole appropriate. In the absence of appropriate injunctive relief requiring Defendants to notify all Class Members that their private information has been breached, Class Members will suffer irreparable harm. Defendants' uniform conduct towards Plaintiff and the other members of the Class makes certification under Rules 23(b)(2) appropriate.

48. Plaintiff also brings this action under Rule 23(b)(3) because the common questions of law and fact identified herein predominate over questions of law and fact affecting individual members of the Class. Indeed, the predominant issues in this class are whether Defendants have violated the law by their unauthorized, inappropriate and undisclosed invasion of privacy, and by their remote access and transmission of communications and information secretly obtained, and by their intentional unauthorized access and use of electronic and computer communications and information. Certification under Rule 23(b)(3) is appropriate because:

a. by virtue of the Hell spyware's clandestine nature as described in this complaint, individual Class Members may not be aware that they have been wronged and are thus unable to prosecute individual claims or take appropriate steps to protect their private information;

b. concentration of the litigation concerning this matter in this Court is desirable;

c. the claims of the representative Plaintiff are typical of the claims of the members of the purported class;

d. a failure of justice will result from the absence of a class action; and

e. the difficulties likely to be encountered in the management of this class action are not great.

## SUBSTANTIVE ALLEGATIONS

49. Details of Uber's spyware code-named Hell emerged publically on or around April 12, 2017 in the form of national news reports.

50. Prior to the April 12, 2017 news reports, Uber actively concealed the existence and scope of its Hell spyware.

51. The Washington Post chronicled the history of Uber's Hell spyware during a series of 2017 articles:

> April 12
>
> According to a report by The Information, Uber operated a top-secret program known as "Hell," which sought to identify drivers for Uber competitor Lyft. The program not only helped Uber in locating Lyft drivers, potentially giving Uber a competitive advantage, the report said, but could also identify which Lyft drivers also drove for Uber. Those drivers would then be singled out for special driver-retention efforts, meaning that they were treated differently from Uber's most loyal workers. Legal analysts said the program could be viewed as an example of an "unfair business practice," which could land Uber in court.
>
> April 14
>
> California regulators said that Uber may be subject to more than $1 million in fines after the company repeatedly failed to take action against drivers that passengers said were driving drunk. Uber investigated only 13 percent of passenger reports about drunken driving, according to California's Public Utility Commission. Uber has promoted its ride-hailing service, in part, by arguing that it reduces drunken driving by keeping inebriated passengers from getting behind the steering wheel.
>
> Brian Fung, *From #deleteUber to 'Hell': A short history of Uber's recent struggles*, THE WASHINGTON POST (April 18, 2017), available at http://wapo.st/2nSRGqF?tid=ss_tw.

52. Amir Efrati, writing for THE INFORMATION, described Uber's Hell spyware as follows:

> As the ride-sharing market was exploding in the U.S. between 2014 and the early part 2016, Uber had an advantage over Lyft that helped Uber maintain its lead, The Information has learned. Thanks to a secret software-based effort within Uber called "Hell," Uber could track how

many Lyft drivers were available for new rides and where they were, according to a person who was involved in the program and a person who was briefed about it.

More importantly, “Hell” showed Uber employees which of the tracked drivers were driving for both Lyft and Uber, helping Uber figure out how to lure those drivers away from its rival. That’s a crucial edge in a business where finding enough people to drive is a constant battle.

THE TAKEAWAY

The revelation of a controversial Uber program aimed at hurting rival Lyft could further complicate CEO Travis Kalanick’s attempt to lead Uber out of its deepening cultural and management crisis. It also opens up the company to potential legal claims.

Only a small group of Uber employees, including top executives such as CEO Travis Kalanick, knew about the program, said the person who was involved in it. Not even Uber’s then-powerful “general managers” who ran the business in individual cities were supposed to know about it.

The program, part of the company’s competitive intelligence, or “COIN,” group, was referred to as “Hell” because it paralleled Uber’s dashboard of Uber drivers and riders known as “God View,” or “Heaven.”

“Hell” was discontinued sometime in the early part of 2016, this person said. This person asked for anonymity because they aren’t authorized to discuss Uber’s internal matters. A spokesman for Uber said the company wouldn’t publicly discuss its internal processes. Lyft said in a statement: "We are in a competitive industry. However, if true, these allegations are very concerning."

Revelation of the program could open up Uber to possible civil legal claims by Lyft, according to lawyers from two law firms that have represented Uber on other matters. Such potential state and federal claims could include “breach of contract”; “unfair business practices”; misappropriation of trade secrets; and a civil violation of the federal Computer Fraud and Abuse Act because of the way Uber allegedly accessed information from Lyft. Such an action could give Lyft the ability to probe certain Uber business practices in court. Antitrust claims also are a possibility if Uber used Hell to help maintain its market power over Lyft—it generates between 70% to 85% of ride-hailing app revenue versus Lyft in key U.S. cities, according to third parties and people inside the companies—these lawyers said.

The public disclosure of Hell and Mr. Kalanick's involvement with it also could make it harder for him to pull Uber out of a deepening cultural and management crisis that started in mid-February. Four of his 13 direct reports have resigned because of conflicts with Mr. Kalanick or because their past behavior was questioned. Mr. Kalanick, despite losing credibility with employees and executives throughout his company because of a variety of revelations, has said he is determined to continue as CEO, albeit with help from a COO he is trying to hire.

Spoofed Riders

Uber and Lyft have waged a war for market share in the U.S. since 2012, when Uber launched UberX, a lower-cost version of its ride-hailing service that let most anyone use their car to pick up Uber riders. UberX was similar to Lyft, which had launched a month earlier. Uber leveraged its early lead in riders, thanks to a high-end "black car" version of the service that began three years earlier, to capture market share against Lyft.

In 2014, Lyft expanded its operations from 20 cities to 65 cities, covering most major U.S. metro areas—places where Uber had already been operating for some time. Lyft's market share was thus small but the company was able to take advantage of the demand for, and awareness of, ride-hailing that Uber had generated previous to Lyft's entrance.

A key weapon in the war between the companies was getting enough drivers so that riders don't have to wait long for a ride. Recruiting drivers through advertising and other marketing has been Uber's top operating expense, judging by confidential financial statements 2015 seen by The Information. That expense easily could have reached $1 billion in 2016, assuming a steady rate of growth.

Hell started like this: Uber created fake Lyft rider accounts and used commonly available software to fool Lyft's system into thinking those riders were in particular locations, according to the person. (That in and of itself is a violation of Lyft's terms of service, which prohibits users from "impersonat[ing] any person or entity," which Lyft riders must agree to when they open the app.)

The spoofed Lyft accounts made by Uber then could get information about as many as eight of the nearest available Lyft drivers who could accommodate a ride request. Uber made sure that in each city where it was competing with Lyft, the fake rider locations were organized in a grid-like format so that it could view the entire city.

In other words, Uber could see, nearly in real time, all of Lyft's drivers who were available for new rides—and where those drivers were located. That also allowed Uber to track the prices Lyft would offer to riders for certain trips, and how many cars were available to pick up riders at a particular time in one city or another.

Lyft's Flaw

But Uber executives realized there was a vulnerability in Lyft's system. The information about the nearby Lyft drivers included a special numbered ID, or token, that was tied to each individual driver. That ID remained consistent over time. So Uber could identify the same drivers again and again no matter where they were in a city. Thus, it learned some of those drivers' habits, such as what time of day or what days of the week they would run the Lyft app. (Uber constantly changes the IDs of its drivers for the Uber app so they can't be tracked in the same way, said the person involved with Hell.)

Here's the critical part of Hell: Because Uber tracked Lyft's drivers over time, it was able to figure out which of them were driving for Uber too, because it would be able to match the locations of its own drivers with those of Lyft. In many cities, more than 60% of Lyft's drivers also drive for Uber because they want to maximize their earnings. (As of a year ago, Lyft said it had about 315,000 drivers.) Uber thus had specific identities and contact information for the majority of Lyft's weekly or monthly active drivers in a particular place. "We achieved ground truth," said the person involved in the program.

Armed with data about when and where Lyft's drivers were operating, Uber aimed to sway them to work only for Uber instead, this person said. One way was to give them special financial bonuses for reaching a certain number of rides per week.

Uber employees involved with the Hell program passed along a list of drivers that should be targeted by the city general managers, who oversaw driver bonus budgets at that time.

Another goal of the program was to make sure Uber steered rides more reliably to Uber drivers who were also available on the Lyft network than to those who weren't, this person said. In other words, if there were several Uber drivers near an Uber rider but one of those drivers was also frequently available on the Lyft network, as seen by the Hell program, Uber's ride-dispatch team was supposed to "tip" that ride request to the driver who was "dual apping," or typically looking for riders through both the Lyft and Uber apps, sometimes by using two different smartphones at the same time.

> The person involved in the program called it "privileged dispatch" and said Uber aimed to use that to squeeze Lyft's supply of drivers. This person didn't know how much the ride-dispatch team used data derived from Hell as part of its calculations. An Uber spokesman said the company does not give preference to "dual-apping" drivers.
>
> "Hustle"
>
> It's unclear if anyone at Uber quantified how helpful Hell was to its business overall, but the program got information about Lyft's network across the country, said the person who was involved with it. During meetings with the small group of people involved in Hell, Mr. Kalanick would often praise the team for the work they were doing and how well it fit into Uber's culture of "hustle" in order to win.
>
> While it's hard to estimate the potential impact of Hell on Lyft, even after the program was shut down, Uber could derive value from knowing which of its drivers were active drivers for Lyft generally, at least for a period of time. "The damage was done," this person said.
>
> Uber and Lyft have other ways of finding out which of their drivers might be driving for the competition. For instance, Lyft can see whether certain of its drivers—those who use Android-powered smartphones—also have the Uber app installed on their phone. (The Android operating system allows app developers to "scan" the phones to see what other apps are on them.) The iPhone is different. Apple stopped allowing app scanning on iPhones starting in mid-2015. But Hell gave Uber much more valuable data.
>
> Hell was overseen by several employees, including a product manager and data scientists who had special access to a room at Uber's headquarters in San Francisco, where the intel on Lyft's drivers was collected via computers that had the spoof accounts, this person said.
>
> Some at Uber might argue that some drivers benefited from Uber's surveillance of Lyft because they made more money when Uber decided to boost their bonuses or give them more rides. But the drivers who benefited most were those who showed less loyalty to Uber. Also, the destruction of Lyft would be bad for drivers in the long run. Lyft's presence in the market has ensured greater bonuses overall, though those may need to disappear if either company wants to make a profit.
> …
> Amir Efrati, *Uber's Top Secret "Hell" Program Exploited Lyft's Vulnerability*, THE INFORMATION (April 12, 2017), available at https://www.theinformation.com/ubers-top-secret-hell-program-exploited-lyfts-vulnerability.

53. Upon information and belief, all of the information and allegations contained in the article quoted in the preceding paragraph are true and accurate.

54. Starting in 2014 or earlier and continuing into 2016, Uber secretly used the Hell spyware to access computer systems, including servers and smartphones, owned and operated by Plaintiff, Class Members, and Lyft.

55. Upon information and belief, Uber used sophisticated software such as Wireshark or another network analyzer (a "Sniffer") to determine how the Lyft App communicated with Lyft's Computer Communication Servers.

56. Lyft's Computer Communication Servers are a remote storage medium for electronic communications, and constitute an electronic communications system as that term is defined in 18 U.S.C. § 2510(14), in that the servers constitute a "wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."

57. The information, data, and communications transmitted to Lyft's servers constitute electronic communications as that term is defined in 8 U.S.C. § 2510(12), as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."

58. Lyft retains the communications at issue in this case for backup purposes of subsequently retrieving the same in response to, among other things, insurance inquiries, driver review, or valid subpoenas or other government requests. *See, e.g.*, Section 2(B), Lyft Privacy Policy, available at: www.lyft.com/privacy ("Driver's location information and distance travelled is necessary for calculating charges and insurance for Lyft rides;" is similarly used to "analyze how the Lyft community uses the Lyft Platform," and to comply with appropriate government requests or investigations, *inter alia*); https://thehub.lyft.com/blog/2016/1/22/drivinghistory (retaining such information to provide detailed "Driver Stats").

59. As such, the electronic communications that are contained on the server are in "electronic storage" as that term is defined in 18 U.S.C. § 2510(17)(B), in that the servers are "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

60. Finally, Lyft's Computer Communication Servers are secure in that they require a username and password to access, and will only transmit the information at issue in this litigation to users (*i.e.*, riders and drivers) who have created accounts with Lyft and agreed to abide by Lyft's Terms of Service.

61. Upon information and belief, Sniffers allow users to monitor all traffic on a wireless network. Although smartphones running the Lyft App would often connect to Lyft using a cellular network, during times that cellular data functionality was disabled, all Lyft App-related data would be routed through a Wi-Fi Network. Upon information and belief, Uber used Sniffers to monitor communications to and from the Lyft App over Wi-Fi Networks. Through this process, Uber was eventually able to obtain sufficient information about the Lyft App and Lyft's Computer Communication Servers to determine how the systems operated.

62. Lyft drivers used software to communicate with Lyft and Lyft riders. More specifically, Lyft drivers used the Lyft Driver App to communicate with servers over the Internet by transmitting and receiving "packets" of information. A packet is analogous to a physical letter mailed from one address to the other, and the protocol used to transmit the packet is analogous to the physical envelope that holds the letter.

63. Upon information and belief, the Lyft App uses the Hypertext Transfer Protocol ("HTTP") to communicate with Lyft's Computer Communication Servers. HTTP "is an application protocol for distributed, collaborative, and hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web."[2]

64. "HTTP functions as a request–response protocol in the client–server computing model. A web browser, for example, may be the client and an application running on a computer

[2] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

hosting a website may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body."[3]

65. The Lyft App, running on a smartphone, was the user agent.

66. "A web browser is an example of a user agent (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web content."[4]

67. "HTTP is designed to permit intermediate network elements to improve or enable communications between clients and servers. High-traffic websites often benefit from web cache servers that deliver content on behalf of upstream servers to improve response time. Web browsers cache previously accessed web resources and reuse them when possible to reduce network traffic. HTTP proxy servers at private network boundaries can facilitate communication for clients without a globally routable address, by relaying messages with external servers."[5]

68. "HTTP is an application layer protocol designed within the framework of the Internet protocol suite. Its definition presumes an underlying and reliable transport layer protocol, and Transmission Control Protocol (TCP) is commonly used."[6]

69. "The [HTTP] GET method requests a representation of the specified resource. Requests using GET should only retrieve data and should have no other effect. (This is also true of some other HTTP methods.) The W3C has published guidance principles on this distinction, saying, 'Web application design should be informed by the above principles, but also by the relevant limitations.'"[7]

[3] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[4] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[5] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[6] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[7] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol#Request_methods

70. The Lyft Rider App allows Lyft riders to obtain transportation from Lyft drivers such as Plaintiff, whom communicates with Lyft riders with the Lyft Driver App.

71. In order to become a Lyft rider, an individual must create a Lyft account and agree to a set of written terms and conditions.

72. Upon information and belief, after a rider logs into the Lyft Rider App the app sends an HTTP request to Lyft's Computer Communication Servers.

73. Upon information and belief, the HTTP request contains the passenger's Lyft Customer ID, and their current GPS coordinates.

74. Upon information and belief, Lyft's Computer Communication Servers responds to the Lyft Rider App's HTTP request with a list of nearby drivers who were logged in and had affirmatively indicated they were available for specific work (indicating a willingness to drive as one of the following products: Lyft, Shared, Lux, Lyft XL, Lux XL, or Lux Black). This list contains the drivers' Lyft Driver IDs as well as their current GPS coordinates. The list is transmitted to riders through Lyft's Computer Communication Servers.

75. When the Lyft Rider App displays Lyft drivers nearby, it only displays small icons of automobiles and does not display any identifying information such as name, type of vehicle, or license plate number. As such, members of the public and Lyft customers in general do not have access to the locations of specific drivers.

76. After a trip is requested by a rider, a nearby Lyft driver is then given the option to provide transportation to the rider by accepting the dispatch. ("When you get a ride request, you'll see a notification. Tap anywhere to accept.").[8]

77. Lyft drivers must accept a ride request within fifteen (15) seconds or the ride request will be sent to another driver.

78. The identities of nearby Lyft drivers always remain anonymous until the Lyft driver affirmatively permits Lyft to provide basic identifying information by accepting the dispatch.

[8] https://help.lyft.com/hc/en-us/articles/115013080028-How-to-give-a-Lyft-ride#app

79. Prospective riders are only able to see the locations of anonymous Lyft drivers for fifteen (15) seconds before being matched with a specific Lyft driver after the driver has accepted the ride request.

80. When a rider requests a driver through the Lyft Rider App, and after the Lyft driver accepts the fare, the rider then is matched a driver that fits the criteria of their request and are provided with identifying information regarding the driver that is normally unavailable to the public (*i.e.*, license plate number, name, vehicle information, driver rating and the driver's physical appearance). Further, the rider is provided with the location of the driver as displayed on a map as well as the estimated time of arrival to the rider.

81. As such, a single rider is only able to obtain the location, first name, vehicle type, and license plate number of a single Lyft driver such as Plaintiff after both parties contract for transportation services by requesting a ride and accepting the dispatch.

82. Lyft's Rider App is similar to a taxi in that both passengers are aware of the location of the taxi as it approaches to pick them up and, of course, while they are in the taxi during the ride.

83. Only by hacking Lyft's software using the Uber Hell spyware as described throughout, and violating Lyft's Terms of Use, was Uber able to obtain the whereabouts and identities of Plaintiff and the Class.

84. Upon information and belief, Uber has requested Lyft rides using the forged Lyft accounts to obtain unauthorized access to Plaintiff's personal identifying information.

85. In the sending and receiving process, HTTP requests are transmitted using the Transmission Control Protocol (TCP).

86. As discussed, the HTTP request itself is the equivalent of a letter – the communication's material content. The letter (HTTP request) is packaged into an envelope (a TCP packet) to deliver it from one computer to another.

87. While traditional envelopes use physical postal addresses, TCP packets use computer Internet Protocol (IP) addresses. For instance, the Lyft App might have an IP address of 15.15.15.15 and Lyft's Central Communication Servers might have a primary IP address of 16.16.16.16. Routers transmitting TCP packets relay the packets through a number of other servers as they travel across

cellular networks, wireless networks, and other wired networks. IP addresses allow the routers to move the packets from one server to the next until they reach their destination. This is essentially equivalent to a sealed letter traveling between different post offices on route to its final destination.

88. In other words, "Transmission Control Protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP segment is then encapsulated into an Internet Protocol (IP) datagram, and exchanged with peers. … A TCP segment consists of a segment header and a data section. The TCP header contains 10 mandatory fields, and an optional extension field. The data section follows the header. Its contents are the payload data carried for the application. The length of the data section is not specified in the TCP segment header. It can be calculated by subtracting the combined length of the TCP header and the encapsulating IP header from the total IP datagram length (specified in the IP header)."[9]

89. In the present matter, Lyft drivers who are ready to work send digital letters to Lyft. Each letter has a number of components that are directly analogous to a physical letter:

a. The IP address for the driver's smartphone, and the IP address for Lyft's Central Communication Servers (the digital equivalent of return and mailing addresses written on an envelope);

b. The TCP packet (the digital equivalent of the physical envelope);

c. A "letter" contained in the digital envelope reciting the following pieces of personal information: (1) the driver's unique identifier; (2) the driver's precise geolocation; (3) the driver's affirmation that he is currently willing to provide a specific product to a rider; (4) the estimated time of arrival; and (5) the estimated price for the ride.

d. The content assembled in the previous paragraphs constitutes an "electronic communication" is defined by 18 U.S.C. § 2510(12).

90. Upon information and belief, Defendants used network analyzers to detect, copy, and decode the TCP packets sent from Lyft's Central Communication Servers to the Lyft App.

[9] https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure

91. Upon information and belief, Defendants reverse-engineered the communication process and were then able to use the Hell spyware to masquerade as Lyft riders seeking rides. Defendants then created a network of fake Lyft riders, arrayed in a grid overlaying metropolitan areas across the United States. These fake Lyft riders would send forged HTTP requests to Lyft's Central Communication Servers.

92. Upon information and belief, the fake Lyft rider accounts created by the Hell spyware all affirmatively agreed to Lyft's Terms of Service, which provides in part that the Lyft App's users will not:

a. impersonate any person or entity;

b. stalk, threaten, or otherwise harass any person, or carry any weapons;

c. violate any law, statute, rule, permit, ordinance or regulation;

d. interfere with or disrupt the Services or the Lyft Platform or the servers or networks connected to the Lyft Platform;

e. post Information or interact on the Lyft Platform or Services in a manner which is false, inaccurate, misleading (directly or by omission or failure to update information), defamatory, libelous, abusive, obscene, profane, offensive, sexually oriented, threatening, harassing, or illegal;

f. use the Lyft Platform in any way that infringes any third party's rights, including but not limited to: intellectual property rights, copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy;

g. post, email or otherwise transmit any malicious code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or surreptitiously intercept or expropriate any system, data or personal information;

h. forge headers or otherwise manipulate identifiers in order to disguise the origin of any information transmitted through the Lyft Platform;

i. "frame" or "mirror" any part of the Lyft Platform, without our prior written authorization or use meta tags or code or other devices containing any reference to us in order to direct any person to any other web site for any purpose; or

j. modify, adapt, translate, reverse engineer, decipher, decompile or otherwise disassemble any portion of the Lyft Platform or any software used on or for the Lyft Platform;

k. rent, lease, lend, sell, redistribute, license or sublicense the Lyft Platform or access to any portion of the Lyft Platform;

l. use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, scrape, "data mine", or in any way reproduce or circumvent the navigational structure or presentation of the Lyft Platform or its contents;

m. link directly or indirectly to any other web sites;

n. transfer or sell your User account, password and/or identification to any other party

o. discriminate against or harass anyone on the basis of race, national origin, religion, gender, gender identity, physical or mental disability, medical condition, marital status, age or sexual orientation, or

p. cause any third party to engage in the restricted activities above.

93. Upon information and belief, the fraudulent HTTP requests sent by the Hell spyware contained the customer IDs of active Lyft rider accounts, as well as the username and password associated with that ID. Defendants created these forged accounts to gain access to Lyft's Central Communication Servers, which are protected computer systems that require user authentication, in violation of Lyft's Terms of Service.

94. When Lyft's Central Communication Servers received a HTTP request from a forged rider account, they believed that the ride requests were coming from actual Lyft riders, not the Hell spyware. As a result, Lyft's servers transmitted an HTTP response (essentially a response letter)

containing the ID's, on duty status, pricing, and exact locations of nearby Lyft drivers (the "Driver Information"). The data transmitted was provided by Lyft drivers, and was only intended to be delivered to actual nearby Lyft riders.

95. The Hell spyware's functionality is analogous to commercially available "scrapping" software. An example of such web scraping software is Scrapy (https://scrapy.org/). An example of how to use scrapping software to instantaneously harvest vast quantities of data from an unsecured website, Craigslist, is *available at:* http://python.gotrained.com/scrapy-tutorial-web-scraping-craigslist/.

96. Upon information and belief, Defendants created manyfraudulent Lyft rider accounts that were used to gain access to Lyft's Central Communication Servers to access the communications drivers sent to prospective riders.

97. Upon information and belief, Defendants sent forged HTTP requests associated with the forged Lyft rider accounts. Defendants then used the fraudulently received GPS coordinates and driver identifiers to create grid-like detection nets over cities like San Francisco, Los Angeles, and New York. For instance, one forged driver account would transmit an HTTP requests indicate that a Lyft rider was at the Philip Burton Federal Building with GPS coordinates of 37.782 -122.418. Lyft's servers would fall for the deception and transmit back information for all nearby Lyft drivers. Simultaneously, the Hell spyware would also send another set of HTTP requests indicating that a different fake Lyft rider was a few blocks north on O'Farrell Street with GPS coordinates of 37.784 -122.418. Upon knowledge or belief, this process could be (and in fact was) repeated with an arbitrarily large number of fake Lyft accounts, allowing Uber to obtain complete geographic coverage of entire metropolitan areas, and the exact locations of all Lyft drivers and other information.

98. Taxi service geolocation data, unique identifiers, and other datasets have been combined before to glean personal info about drivers and passengers. For example, in 2014 an

analyst used anonymous New York City taxi records cross-referenced pickup and drop-off location coordinates with publically available data to identify the patrons of a strip club.[10]

99. Upon information and belief, Defendants sent hundreds or even thousands of requests every second from the grid-like array of forged Lyft rider accounts, essentially allowing Defendants to monitor the whereabouts of all Lyft drivers in major markets like San Francisco, Los Angeles, and New York in real time.

100. Upon information and belief, Uber used the vast quantities of personal data collected by the Hell spyware to create a historical database, allowing it to retroactively scrutinize the activities of Lyft's drivers. Upon information and belief, Uber used the data collected through its industrial espionage in conjunction with other databases to learn personal details about Lyft drivers including, but not limited to, the drivers' full names, their home addresses, when and where they typically work each day and for how many hours, and where they take breaks. Also upon information and belief, Uber was able to use the data collected to determine the identities of the drivers' rider customers, and relatedly, personal income derived from Lyft.

101. Upon information and belief, Uber's requests for drivers has caused Plaintiff and the Class to "chase" after non-existent fares and create "Prime Time" that are manipulated by Uber through the elimination of drivers (supply) and increased by the number of forged riders (demand). Through this process, Uber is able to manipulate the market, affect fare pricing, and "trick" drivers into "chasing" fares.

102. Lyft implements "Prime time" for passengers to encourage drivers to drive in areas and at times with more demand than usual. As an incentive to drivers to dive in those areas, riders may pay an additional percentage in addition to the normal price.

103. Uber implements its own incentive program similar to Lyft's "Prime Time" to encourage drivers to drive at certain times and locations. Uber's "surge pricing" adjusts the prices of fares to match driver supply to rider demand at any given time. During periods of excessive demand

[10] Chris Gayomali, *NYC Taxi Data Blunder Reveals Which Celebs Don't Tip - And Who Frequents Strip Clubs*, Oct. 2, 2014, available at https://www.fastcompany.com/3036573/nyc-taxi-data-blunder-reveals-which-celebs-dont-tip-and-who-frequents-strip-clubs

when there are many more riders than drivers, or when there are not enough drivers on the road and customer wait times are long, Uber increases its normal fares to attract drivers to drive in those areas.

104. Upon information and belief, in combination of Uber's fake rider accounts affecting Lyft's "Prime Time" pricing scheme and implementing its own "Surge Pricing" scheme, Uber can manipulate the market and affect fares collected by the Plaintiff and Class.

105. As a result of chasing after non-existent fares, Plaintiff and the Class suffered injury and loss in the form of unnecessary fuel consumption, lost time spent driving, and lost economic opportunities in the form of fares assigned to other drivers that would have been assigned to Plaintiff but-for the Uber Hell spyware ride requests.

106. Upon information and belief, Uber implements its own surge pricing scheme to manipulate Uber drivers to drive in specific areas that affect the transportation market including but not limited to Lyft Drivers.

107. Plaintiff and Class Members are Lyft drivers who affirmatively signaled that they were available to transport fare-paying passengers. They did so by opening the Lyft App and swiping a button to go on duty.

108. Upon information and belief, Plaintiff used the Lyft App running on his smartphone to send an HTTP request to Lyft's Computer Communication Servers with his Driver Information. This data was stored on Lyft's Computer Communication Servers.

109. Upon information and belief, the Lyft's Computer Communication Servers also redirected and forwarded Plaintiff's Driver Information to authorized riders in Plaintiff's vicinity seeking transportation.

110. Upon information and belief, Lyft's Computer Communication Servers store the location of every Lyft driver, whether on duty or off duty, every few seconds.

111. Upon information and belief, Uber's computer systems also store the location of every Uber driver, whether on duty or off duty, every few seconds.

112. Upon information and belief, Uber's computer systems also store the location of every Uber rider, whether or not the rider is currently requesting a ride, every few seconds.

113. Upon information and belief, neither Uber nor Lyft ever delete the geolocation data they collect from drivers, at least in part because they consider it valuable to their respective businesses and back-up such information for, *inter alia*, liability purposes.

114. Upon information and belief, the Uber Hell spyware used the above-described technology to send numerous forged HTTP requests to Lyft's Computer Communication Servers which caused it to automatically respond initially with Driver Information it had previously stored in databases and, as Hell's requests continued, redirect/forward Driver Information transmitted directly by Lyft Driver Apps that was intended for actual fare-paying riders nearby. Thus, the Hell spyware allowed Defendants to access Driver Information being transmitted through Lyft's Computer Communication Servers in real time (save for the inherent lag in any computer network) as well as access the Driver Information stored in databases on Lyft's Computer Communication Servers.

115. Upon information and belief, Lyft drivers would begin transmitting their personal information through the Lyft App as soon as they opened the Lyft Driver App and indicated they were available for work. Such information may even be collected when the application is turned off "to identify promotions or service updates in your area." *See*, Section 2(B), Lyft Privacy Policy, *available at:* www.lyft.com/privacy. These transmissions were not limited to times that the Lyft drivers were on public roads. For example, if a Lyft driver activated the app while still in the driveways of their homes, the Hell spyware would provide Uber with the means to discern where Lyft drivers lived.

116. Thus, the information collected with a potentially infinite amount of historical waypoints that Uber intercepted and amassed in real time over several years painting a vivid, intimate, portrait of one's life including, but not limited to, "home" and "work" locations, identity, employment hours, work schedule, and employment history.

117. When logged in to the Lyft Driver App, Plaintiff and the Class consented to share their location, unique identifier, and work availability status, only with Lyft and actual Lyft riders. Upon information and belief, neither Plaintiff nor any member of the Class agreed to share the aforementioned information with Uber.

118. Further, Lyft was the only entity that Plaintiff and the Class allowed to maintain a historical record of their geolocation data. Actual Lyft riders would have no way of keeping such records, especially because the unique identifiers belonging to Lyft drivers is not displayed on the visual display available to riders searching for a driver. Rather, riders only see an icon of a car imposed on a map. Upon information and belief, neither Plaintiff nor any member of the Class agreed to allow Uber to maintain their historical geolocation data.

119. As designed, the Hell spyware enabled Defendants to surreptitiously access, monitor, use, and/or transmit personal information as well as electronic communications and whereabouts in real time, other than the nominal delay attributable to network speed limitations when moving communications across Lyft's servers

120. Upon information and belief, Uber's Hell spyware enabled Uber to engage, and Defendants did in fact engage, in illegal, surreptitious, and unauthorized covert electronic surveillance, intrusion on Plaintiff and Class Members' privacy, seclusion, anonymity, whereabouts, and use of protected private communications.

121. Upon information and belief, Uber's Hell spyware was developed, written, manufactured, assembled, and utilized by Uber for the purpose of allowing Uber to remotely spy on Plaintiff and Class Members, as well as track, access, monitor, and/or transmit electronic communications on Lyft and Class Members' computer systems.

122. Upon information and belief, Uber's Hell spyware was designed to be invisible or generally undetectable to Lyft, Class Members, and law enforcement officials.

123. Upon information and belief, Uber did engage in the conduct described in the preceding paragraphs.

124. Upon information and belief, Uber profited from the Hell spyware in a number of ways.

125. Upon information and belief, Uber used the information gleaned from Hell to direct more frequent and more profitable trips to Uber drivers who also used the Lyft Driver App. By inundating these drivers with Uber fares, Uber was able to discourage drivers from accepting work on the Lyft platform, reducing the effective supply of Lyft drivers available.

126. With the effective supply of Lyft drivers reduced, Lyft customers faced longer wait times. As a result, Lyft riders would cancel the ride requested with Lyft and request a new ride from Uber. In particular, Plaintiff had accepted rides that were subsequently cancelled, those rides were cancelled while Plaintiff had already begun the process to locate and pick up those rides (*e.g.*, he had started driving towards the location of his confirmed fare and expended time and fuel), and it is plausible that those cancellations were the result of the proximity and convenience of Uber drivers as a direct result of Defendants' surreptitious conduct. Over time, this also could reduce rider's loyalty to Lyft, further harming drivers such as Plaintiff and absent Class Members.

127. Upon information and belief, Uber still maintains the data collected using the Hell Spyware on its computer systems. In other words, Uber has not destroyed the ill-gotten data it obtained at the expense of Plaintiff, the Class, and Lyft.

## CAUSES OF ACTION

### COUNT I
### Violation of the Stored Communications Act
### 18 U.S.C. § 2701
### (on behalf of the Class)

128. Plaintiff incorporates all preceding and succeeding allegations by reference as if fully set forth herein.

129. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

130. Defendants violated the Stored Communications Act (the "SCA") by accessing Lyft's servers and obtained communications stored and transmitted through the same.

131. "The Stored Communications Act provides a cause of action against anyone who 'intentionally accesses without authorization a facility through which an electronic communication service is provided... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.'" *Theofel v. Farley-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (citation omitted).

132. The communication in question was in electronic storage when it was unlawfully accessed. The SCA defines "electronic storage" as, *inter alia*, any storage of such communication by

an electronic communication service for the purpose of backup protection of such communication. 18 U.S.C. § 2510(17)(B).

133. The communication is collected and stored for backup purposes and retrieved as needed to respond to government inquiries, insurance evaluations, or analyses of individual drivers, *inter alia*.

134. Defendants' access of the communications in question was unauthorized as neither Plaintiff nor Lyft contemplated or authorized such access of the information by Defendant. Indeed, such access was directly contrary to Lyft's terms of service as Defendant falsely posed as a Lyft rider to gain access to such information. *See*, Section 9, Lyft Terms of Service, *available at:* www.lyft.com/terms.

135. Defendant's access to the stored information is the personal information of the Lyft drivers including Plaintiff and the Class, and is owned by each individual respectively.

136. Accordingly, Defendants have intentionally accessed without authorization a facility through which an electronic communications service is provided and thereby obtained an electronic communication while it was in electronic storage in such system in violation of 18 U.S.C. § 2701(a), entitling Plaintiff and the Class to preliminary and other equitable or declaratory relief, actual damages or statutory damages not less than the sum of $1000, punitive damages, and reasonable attorney's fees and other litigation costs reasonably incurred pursuant to 18 U.S.C. § 2707.

**COUNT II**
**Violation of the California Computer Data Access and Fraud Act**
**Cal. Penal Code § 502 *et seq.***
**(on behalf of the California Subclass)**

137. Plaintiff incorporates all preceding and succeeding allegations by reference as if fully set forth herein.

138. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

139. This cause of action is brought pursuant to the Cal. Penal Code § 502, the California Comprehensive Computer Data Access and Fraud Act ("CDAFA").

140. As detailed above, Defendants accessed information stored in Lyft's service to gather intelligence on Lyft drivers, divert Lyft drivers and ultimately potential Lyft riders from Plaintiff, the

Class, and Lyft, and obtain a competitive advantage over Lyft at the expense of Plaintiff and the Class.

141. The access was without permission, contrary to the Lyft Terms of Service, and surreptitious in that the spyware was not detectable by any individual Class Member including Plaintiff.

142. Such conduct violates numerous provisions of the CDAFA including, but not limited to, Cal. Penal Code § 502(c)(1), knowing access, without permission, use of data, in order to wrongfully control or obtain money; § 502(c)(2) taking or making use of data from a computer system without permission; and § 502(c)(7) providing the a means of accessing computer system without permission.

143. As owner of his personal data which Defendants accessed in violation of the CDAFA, Plaintiff is entitled to seek compensatory damages and equitable relief. Cal. Penal Code § 502(e)(1).

**COUNT III**
**Violation of the California Unfair Competition Law**
**Cal. Bus. & Prof. Code § 17200 *et seq.***
**(on behalf of the California Subclass)**

144. Plaintiff incorporates all preceding and succeeding allegations by reference as if fully set forth herein.

145. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

146. This cause of action is brought pursuant to California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* ("the UCL").

147. Defendants engaged in unlawful and unfair conduct under the UCL through its unlawful, unethical, and immoral use of its Hell spyware as described more fully herein.

148. Defendants' actions and practices constitute "unlawful" business practices in violation of the UCL because, among other law, Defendants violated the following statutes:

a) The SCA, as detailed in Plaintiff's first cause of action;

b) The CDAFA, as detailed in Plaintiff's second cause of action;

c) The Economic Espionage Act (18 U.S. Code § 1832); and

d) The Computer Fraud and Abuse Act (18 U.S.C. § 1030).

149. Moreover, as detailed in Count IV, Defendants' conduct is contrary to the provisions of the California Constitution.

150. Defendants' actions and practices constitute "unfair" business practices because Defendants' practices, as described throughout this complaint, offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

151. Defendants' actions and practices constitute "unfair" business practices because Defendants' practices, as described throughout this complaint, represent "conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel-Tech Commc'ns, Inc. v. L. A.s Cellular Tel. Co.*, 20 Cal. 4th 163, 186 (Cal. 1999).

152. Because of the surreptitious nature of Defendants' conduct and no assurances Defendants will not re-implement their spyware technology, injunctive relief is necessary to protect Class Members and future Lyft drivers. Moreover, Defendants have not destroyed the wrongfully obtained data concerning the personal and private movements of Plaintiff and the Class such that injunctive relief is necessary to ensure such information will not be used or disseminated in the future, harming competition and unlawfully invading individual privacy rights.

153. Additionally, as a direct and proximate result of Defendants' violations, Plaintiff and members of the Class have suffered and continue to suffer injury in fact and lose money or property as a result of Defendant's conduct.

154. Specifically but without limitation, Plaintiff accepted rides that were subsequently cancelled, some of those rides were cancelled while Plaintiff had already begun the process to locate and pick up those rides, and it is plausible that those cancellations were the result of the proximity/convenience presented by Uber drivers. In cancelling their rides as a direct result of Defendants' conduct, at a minimum, Plaintiff suffered concrete monetary loss in the form of fuel expended to seek and locate those fares for which he was not compensated, lost time, and lost economic opportunity in driving legitimate fare-paying passengers.

155. Plaintiff and the Class have also suffered monetary damage in the form of staunched

demand for Lyft services. By diverting dual-app drivers to Defendants' application and decreasing the availability of Lyft drivers, Defendants have unlawfully deterred riders from using Lyft services and deprived Plaintiff and the Class from earning income.

156. Plaintiff, on behalf of himself and the Class, seeks: (a) injunctive relief in the form of an order requiring Defendant to cease the acts of unfair competition alleged herein and purge all ill-gotten personal and private information from Defendants' computers and records; (b) restitution; (c) declaratory relief; and (d) attorney fees and costs pursuant to Cal. Code Civ. P. § 1021.5, *inter alia*.

**COUNT IV**
**Invasion of Privacy**
**Cal. Const. Art. I, § 1**
**(on behalf of the California Subclass)**

157. Plaintiff incorporates all of the proceeding paragraphs herein.

158. The California Constitution declares that:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Cal. Const. Art. I, § 1.

159. As described herein, Defendants engaged in conduct that invaded Plaintiff's and Class Members' privacy interests, including, but not limited to, obtaining private communications not intended for Defendants and monitoring their whereabouts.

160. The Hell spyware invaded both types of privacy interests recognized in California law: "(1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ('autonomy privacy')." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35 (Cal. 1994).

161. The Supreme Court has recognized a reasonable expectation to privacy in movements, including cell-site location information similar to that in question here despite dissemination to third parties for business purposes. *Carpenter v. United States*, 138 S.Ct. 2206 (2018).

162. Indeed, "[a]s with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Id*. at 2217 (quotation omitted).

163. Plaintiff and Class Members had a reasonable expectation of privacy as to the interests invaded.

164. Plaintiff and Class Members never consented to Uber's tracking of their location information or movements.

165. Plaintiff and Class Members never consented for Lyft to share their location data to the general public or fraudulent customers.

166. Plaintiff and Class Members only shared their identities and locations with Lyft, their employer, and individual customers on an individual, transactional basis after accepting individual ride requests. Plaintiff and Class Members only consented to sharing this information with bona fide rider customers during that single transaction/ride. To the broader public using the Lyft Rider App, Plaintiff and Class Members remained anonymous as they appeared only as generic automobile icons for a matter of seconds.

167. Through its Hell spyware, Uber hacked Lyft's software and servers, breaching not only Lyft's Terms of Use but also societal norms, and was able to compile vast amounts of information about Plaintiff and Class Members, including, but not limited to, their first name, type of vehicle driven, license plate number, and precise location over long periods of time.

168. Plaintiff and Class Members had a reasonable expectation that this information was private and would remain private. Indeed, other than Uber through its Hell spyware, this information remains private to this today to everyone other than Lyft.

169. When Defendants accessed such information from Lyft's servers, it invaded Plaintiff's and the Class's reasonable expectation of privacy in the whole of their physical movements. *Id*. at 2219.

170. By hacking Lyft's software, Uber's Hell spyware was able to track the same driver over long periods of time using a static identification number. It was only over time that Plaintiff and Class Members' private movements became valuable as it could be matched with Uber's own

location data or cross-referenced against public and commercial databases with precision.

171. By hacking Lyft's software and tracking Lyft drivers by their static identification number, Uber was able to glean much more information that it could have as a prospective rider learning the location of anonymous Lyft drivers for fifteen seconds or a bona fide Lyft rider customer one trip at a time.

172. Plaintiff could not have expected Defendants' egregious breach of commercial practices in violating the Lyft Terms of Service and circumventing the protected servers collecting his personal information for the purposes of obtaining a competitive advantage over Plaintiff, the Class, and Lyft.

173. Defendants' invasion of Plaintiff and Class Members' privacy interests was serious and sustained over several years. As in *Carpenter*, "this case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id*. at 2220.

174. Individual rider customers only knew Plaintiff and Class Member's location for a very brief period of time: as the driver was approaching for pickup and during the ride itself. Conversely, Uber's invasion of Plaintiff and Class Members' privacy interests was sustained and allowed Uber to build detailed portraits of individuals' lives by tracking their movements.

175. Plaintiff and Class Members never consented to sharing any of their private information with Uber.

176. Plaintiff and Class Members never consented to sharing any of their private information with the general public.

177. Plaintiff and Class Members never consented to sharing any of their private information with every Lyft customer.

178. Plaintiff and Class Members only consented to sharing their private information with Lyft, their employer, while working and – after affirmatively accepting the ride request – with a single Lyft rider customer for a brief period before their pickup and throughout the duration of their ride.

179. Thus, Plaintiff and Class Members never consented to sharing any of their private

information with perfect strangers other than a bona fide customer seeking their services at that time and only for a short period.

180. This is no different from any other employee in a service business sharing their current location information with a customer for a short period. A barista at a coffee shop inherently shares their location information with a customer while ordering – the customer sees the barista standing there. While a court clerk shares their location information with the courier standing in front of them, they do not share their location information with attorneys filing motions electronically.

181. Defendants' invasion of Plaintiff and Class Members' privacy interests caused Plaintiff and Class Members to suffer injury and damages.

182. The intentional and deliberate invasion of privacy as referenced herein constituted wanton, willful, and malicious conduct justifying an award of punitive damages against these Defendants.

**PRAYER FOR RELIEF**

Plaintiff, on behalf of himself and the Class, prays for relief as follows:

A. For an order certifying that the action may be maintained as a class action and appointing Plaintiff and the undersigned counsel to represent the Class in this litigation;

B. For an order declaring that Defendants' acts and practices constitute violations of the SCA, CDAFA, and UCL;

C. For a permanent injunction enjoining Defendant from continuing to harm Plaintiff and members of the Class and the public, and violating California and federal law in the manners described above;

D. For a permanent injunction requiring the destruction of the data collected using the Hell Spyware;

E. For restitution;

F. For actual, compensatory, statutory, punitive, and nominal damages where permitted;

G. For reasonable attorneys' fees and the costs of the suit; and

H. For all such other relief as this Court may deem just and proper and may be available at law or equity.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands trial by jury of all claims so triable.

Dated: July 18, 2018

By: /s/ Caleb Marker

Michael A. McShane, SBN 127944
Mark E. Burton, Jr., SBN 178400
AUDET & PARTNERS, LLP
711 Van Ness, Suite 500
San Francisco, CA 94102-3229
Tel: 415.568.2555 | Fax: 415.568.2556
mmcshane@audetlaw.com
mburton@audetlaw.com

Caleb Marker, SBN 269721
ZIMMERMAN REED LLP
2381 Rosecrans Avenue, Suite 328
Manhattan Beach, CA 90245
Tel: 877.500.8780 | Fax: 877.500.8781
caleb.marker@zimmreed.com

*Attorneys for Plaintiff and the Class*